UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,505	12/26/2000	Gordon Edward Larose	77805-29	1765

7380 7590 06/04/2004

SMART & BIGGAR/FETHERSTONHAUGH & CO.
P.O. BOX 2999, STATION D
55 METCALFE STREET
OTTAWA, ON K1P5Y6
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	5

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/745,505	LAROSE, GORDON EDWARD	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on December 26, 2000. Claims 1 – 33 were received for consideration. No preliminary amendments for the claims were field. Currently claims 1 – 33 are being considered.

Information Disclosure Statement

2. An initialed and dated copy of applicant's IDS form 1449, Paper No. 2, is attached to the Office action.

Claim Objections

3. Claim 1 is objected to because of the following informalities: The first 2 limitations of claim 1 need to be concluded with a semicolon, ";" and not a comma. Appropriate correction is required.

3. Claim 26 is objected to because of the following informalities: Claim 26 is said to depend on "claim 26." This is assumed to be actually dependent on claim 25. Appropriate correction is required.

4. Claim 26 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 26 describes embedding electronic cash and initiating an interaction with a banking server, which is separate from the function of claim 25, and therefore fails to limit the parent claim.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, 4-12, 14-16, 18-25, 27-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Guthery (U.S. Patent 6,308,270).

Regarding claim 1, Guthery discloses:

A method of producing an executable instance of a software application in a secure hardware adjunct where secure processing is performed, the method comprising the steps of:

providing a non-executable form of a software application to the secure hardware adjunct (column 1 lines 33 – 42, column 4 lines 31 – 45);

providing sensitive functions to the secure hardware adjunct (Figure 2 items 104, 105, column 4 lines 31 – 65);

transforming the non-executable form of the software application into an executable form of the software application in the secure hardware adjunct (column 4 line 65 – column 5 line 4);

integrating the sensitive functions with the executable form of the software application in the secure hardware adjunct to produce an executable instance of the software application (Figure 2 items 104, 105, column 4 lines 31 – 65); and

outputting the executable instance of the software application to a digital appliance (Figure 2 item 106, column 4 line 65 – column 5 line 4).

Regarding claim 27, Guthery discloses:

A secure hardware adjunct comprising:

a processor where secure processing can be performed, read only memory connected to said processor (column 3 lines 42 – 58);

random access memory connected to said processor (column 3 42 – 58);

input and output paths for communication between the processor and a digital appliance (column 3 line 58 – column 4 line 30);

a secure housing covering the processor, the read only memory and the random access memory, the secure housing being resistant to tampering and observation of data and algorithms in the processor, the read only memory and the random access memory (column 3 lines 42 – 58);

the processor, upon being provided with a non-executable form of a software application and sensitive functions on the input path, transforms the non-executable form of the software application into an executable form of the software application; integrates the sensitive functions with the executable form of the software application to produce an executable instance of the software application; and outputs on the output path the executable instance of the software application to the digital appliance (Figure 2 items 104, 105, 106, column 1 lines 33 – 42, column 4 line 31 – column 5 line 4).

Regarding claim 31, Guthery discloses:

Computer readable medium storing processor executable instructions for use in producing an executable instance of a software application in a secure hardware adjunct where secure processing is performed, the secure hardware adjunct being provided with a non-executable form of a software application and sensitive functions, the processor executable instructions when loaded at a processor in the secure hardware adjunct adapt said processor to:

transform the non-executable form of the software application into an executable form of the software application (column 4 line 65 – column 5 line 4);

integrate the sensitive functions with the executable form of the software application to produce an executable instance of the software application (Figure 2 items 104, 105, column 4 lines 31 – 65); and

output the executable instance of the software application to the digital appliance (Figure 2 item 106, column 4 line 65 – column 5 line 4).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 wherein the sensitive functions comprise one or more of the following:

i. a digital rights management algorithm;

ii. a user authentication algorithm;

iii. a user contract determination algorithm;

iv. a cryptographic key request and download algorithm; and

v. an algorithm for scanning the digital appliance for appliance-specific identifiers (column 5 lines 4 – 13).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 wherein the secure hardware adjunct is implemented by one of the following:

i. a secure integrated circuit on a motherboard of the digital appliance;

ii. a secure integrated circuit on an expansion board of the digital appliance;

iii. an external device connected to the digital

appliance through an external port;

iv. a smart card and smart card reader; or

v. a component of a wireless Internet-enabled handheld device (column 3 line 59 – column 4 line 13).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the step of: following the transforming step, varying the positioning of binary instructions of the executable form of the software application in the secure hardware adjunct (column 4 line 65 – column 5 line 4).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 wherein the step of transforming includes the step of using a private decryption key stored in the secure hardware adjunct to decrypt the non-executable form of the software application (column 5 lines 4 – 13).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the step of executing the executable instance of the software application in the digital appliance immediately upon completion of the outputting step (Figure 2 item 106, column 4 line 65 – column 5 line 4).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the steps of:

inspecting the digital appliance for environmental data (column 2 lines 1 – 29, column 4 lines 31 - 45);

providing the environmental data to the secure hardware adjunct (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the step of inspecting the secure hardware adjunct for environmental data appliance (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the steps of:

executing the executable instance of the software application in the digital appliance (Figure 2 item 106, column 4 line 65 – column 5 line 4);

verifying the status of the secure hardware adjunct (column 4 lines 31 – 65);

if the status of the secure hardware adjunct is changed, then ceasing the execution of the executable instance of the software application (Figure 2, column 4 lines 31 – 45).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the steps of:

scanning the digital appliance for identification data (column 2 lines 1 – 29, column 4 lines 31 - 45);

providing the identification data to the secure hardware adjunct (column 2 lines 1 – 29, column 4 lines 31 - 45);

integrating the identification data with the executable form of the software application (column 2 lines 1 – 29, column 4 lines 31 - 45); and

wherein the outputted executable instance of the software application further incorporates the identification data (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 wherein the step of integrating includes the following:

selecting, from among the provided sensitive functions, a subset of sensitive functions to be integrated into the executable form of the software application (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 22 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 wherein the non-executable form of the software application cannot be rendered executable without the integration of the sensitive functions (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 23 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the steps of:

requesting the entry of a personal identification number (column 5 lines 3 – 13); and

executing the executable instance of the software application only if the entered personal identification number matches a personal identification number integrated into the executable instance of the software application (column 5 lines 3 – 13).

Claim 24 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 further including the steps of:

providing encrypted data files associated with the non-executable form of the software application to the secure hardware adjunct (column 5 lines 3 – 13);

decrypting the encrypted data files in the secure hardware adjunct (column 5 lines 3 – 13).

Claim 25 is rejected as applied above in rejecting claim 26. Furthermore, Guthery discloses:

The method of claim 1 further including the steps of:

authorizing the rights of a user to access the executable instance of the software application and only proceeding to the transforming, binding and outputting steps if the user's rights have been authenticated (Figure 2 item 106, column 4 line 65 – column 5 line 4).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Guthery discloses:

The secure hardware adjunct of claim 27 wherein said processor is connected to a smart card reader (column 4 lines 4 – 30).

Claim 29 is rejected as applied above in rejecting claim 27. Furthermore, Guthery discloses:

The secure hardware adjunct of claim 27 wherein said processor comprises part of an integrated circuit on an expansion board of the digital appliance (column 4 lines 4 – 30).

Claim 30 is rejected as applied above in rejecting claim 27. Furthermore, Guthery discloses:

The secure hardware adjunct of claim 27 wherein the sensitive functions comprise one or more of the following:

i. a digital rights management algorithm;

ii. a user authentication algorithm;

iii. a user contract determination algorithm;

iv. a cryptographic key request and download algorithm; and

v. an algorithm for scanning the digital appliance for appliance-specific identifiers (column 5 lines 4 – 13).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Guthery discloses:

The computer readable medium of claim 31 wherein the secure hardware adjunct is implemented by one of the following:

i. a secure integrated circuit on a motherboard of the digital appliance;

ii. a secure integrated circuit on an expansion board of the digital appliance;

iii. an external device connected to the digital appliance through an external port;

iv. a smart card and smart card reader; or

v. a component of a wireless Internet-enabled handheld device (column 3 line 59 – column 4 line 13).

Claim 33 is rejected as applied above in rejecting claim 31. Furthermore, Guthery discloses:

The computer readable medium of claim 31 wherein the sensitive functions comprise one or more of the following:

i. a digital rights management algorithm;

ii. a user authentication algorithm;

iii. a user contract determination algorithm;

iv. a cryptographic key request and download algorithm; and

v. an algorithm for scanning the digital appliance for appliance-specific identifiers (column 5 lines 4 – 13).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Guthery discloses:

The method of claim 8 further including the step of:

embedding the environmental data in the executable instance of the software application, the environmental data functioning upon execution of the software application to restrict execution to the digital appliance (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 10 is rejected as applied above in rejecting claim 8. Furthermore, Guthery discloses:

The method of claim 8 further including the steps of:

prior to the integrating step, using the environmental data to select, from among the provided sensitive functions, a subset of sensitive functions to be integrated into the executable form of the software application (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 11 is rejected as applied above in rejecting claim 8. Furthermore, Guthery discloses:

The method of claim 8 further including the steps of:

following the outputting step, re-inspecting the digital appliance for environmental data (column 2 lines 1 – 29, column 4 lines 31 – 45);

executing the executable instance of the software application only if the environmental data provided to the secure hardware adjunct matches the environmental data located during the re-inspecting step (Figure 2 item 106, column 4 line 65 – column 5 line 4).

Claim 12 is rejected as applied above in rejecting claim 8. Furthermore, Guthery discloses:

The method of claim 8 wherein the environmental data consists of information about one or more of the following:

i. the digital appliance executing the executable instance of the software application;

ii. a user;

iii. the secure hardware adjunct; and

iv. network accessible resources (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 14 is rejected as applied above in rejecting claim 8. Furthermore, Guthery discloses:

The method of claim 8 wherein the secure hardware adjunct is a bus master, capable of inspecting the digital appliance independent of any hardware or software contained in the digital appliance (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 15 is rejected as applied above in rejecting claim 8. Furthermore, Guthery discloses:

The method of claim 8 wherein the inspecting and providing steps are performed under the control of an auxiliary external software program appliance (column 2 lines 1 – 29, column 4 lines 31 - 45).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Guthery discloses:

The method of claim 18 further including the step of:

passing control over the executable instance of the software application to an integration framework software process, so that said process might provide recovery action beyond simply stopping the application (Figure 2 item 106, column 4 line 65 – column 5 line 4).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3, 13, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthery (U.S. Patent 6,308,270).

Claim 3 is rejected as applied above in rejecting 1. Guthery does not disclose the downloading of sensitive functions from an Internet server. Guthery does make reference to the smart card having the ability to communicate over a local area or a wide area network via the Internet (column 4 lines 10 – 13). Guthery can obtain sensitive functions from the host in the present embodiment, which is for one host and one smart card. However, in cases where multiple hosts and smart cards were present, an Internet server would reduce the processing load on the host by storing the sensitive functions, in an encrypted mode for security purposes, for subsequent downloading by the secure hardware adjunct. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to store the sensitive functions on an Internet server to reduce the processing load on the host and to more efficiently and securely distribute the sensitive functions.

Claim 13 is rejected as applied above in rejecting claim 1. Guthery does not disclose the downloading of environmental data from an Internet server. Guthery does make reference to the smart card having the ability to communicate over a local area or a wide area network via the Internet (column 4 lines 10 – 13). Guthery can obtain environment data from the host in the present embodiment, which is for one host and one smart card. However, in cases where multiple hosts and smart cards were present, an Internet server would reduce the processing load on the host by storing the environmental data, in an encrypted mode for security purposes, for subsequent downloading by the secure hardware adjunct. The secure hardware adjunct does have the capability to encrypt and decrypt data (column 5 lines 3 – 13), and can decrypt the encrypted environmental data which is used to authorize the user. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to store the environmental data on an Internet server to reduce the processing load on the host and to more efficiently and securely distribute the environmental data.

Claim 17 is rejected as applied above in rejecting claim 1. Furthermore, Guthery discloses:

The method of claim 1 wherein the step of providing a non-executable form of a software application to the secure hardware adjunct includes the following steps:

embedding a private decryption key in the secure hardware adjunct (column 5 lines 3 – 13);

encrypting the software application with a public encryption key corresponding to the private decryption key to produce a non-executable form of the software application (column 5 lines 3 – 13).

Guthery does not explicitly teach the downloading the non-executable form of the software application from an Internet server to the secure hardware adjunct. Guthery does make reference to the smart card having the ability to communicate over a local area or a wide area network via the Internet (column 4 lines 10 – 13). In the present embodiment the non-executable form of the software application is received from the host. However, in cases of updates and other applications that are stored on a server, the secure hardware adjunct would have the ability to retrieve it as it already communicates with a host, which could be a server. The capability to communicate with an Internet server is present in the disclosure by Guthery, and it cases where updates to software or widespread releases of software are available, an Internet server would be best suited to distribute the software and/or updates. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to store the non-executable on an Internet server for easier distribution to multiple secure hardware adjuncts more efficiently and securely.

7. Claims 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Guthery (U.S. Patent 6,308,270) in view of Kawan (U.S. Patent 6,289,324).

Guthery does not explicitly teach using the secure hardware adjunct for the purpose of interacting with a bank server, and embedding the secure hardware with electronic cash. Guthery does teach a smart card with a microprocessor capable of communicating via the Internet with a server. Kawan teaches using a smart card for the purpose of financial transactions and have electronic cash, which can be decremented as required by a server or an external terminal (column 4 lines 48 – 63). Kawan states that "there is a need for a smart card that offers enhanced convenience when assisting a customer in executing a transaction" (column 2 lines 12 – 15). Therefore it would have been obvious on one of ordinary skill in the art to use the invention of Kawan in conjunction with Guthery to allow a user to purchase a software application and download the application using the same smart card, for the enhanced convenience that Kawan discusses, in addition to the security of downloading the application directly onto the smart card and not through an intermediary source.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 703-305-8892. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

KA
05/27/2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100